International Journal of Recent Technology and Engineering (IJRTE)
ISSN: 2277-3878 (Online), Volume-8 Issue-2, July 2019

FPGA Implementation of Encryption and Decryption of a Message using Optimized Reconfigurable Reversible Gate

K. Rajesh, G. Umamaheswara Reddy

Abstract*: The prime incentive to learn reversible computation is that it is the best efficient way to reduce heat dissipation than any other conventional methods. The major condition for reversibility is that there is a one-to-one connection between each input and output vectors and it has received a huge significance because of there no information loss throughout the reversible computation which results in reduces the power dissipation. Here, we proposed the design of encryption/decryption of the data schemes by using reversible computing. In this regard, a basic building block is designed for encryption design is simply cascading of a 4-bit reversible gates and it is performed every 4-variable reversible functions, for this intention a new reconfigurable reversible gate (RRG) is proposed and is designed with the use of basic reversible gates like NOT gate, CNOT gate, Toffoli gate, and Fredkin gates. In this work, the encryption/decryption of an 8-bit data is proposed and the Simulation results of encryption/decryption of the circuits using reversible gates are also presented. The gate count, delay, constant inputs, and the garbage outputs are calculated. The complete Simulation and the synthesis process can be finished with the Xilinx ISE 14.7 version and it is dumped on the FPGA Zynq board.

Index Terms*: Decryption, Encryption, FPGA- Field Programmable gate array, Reversible Computation, RRG - Reconfigurable Reversible Gate.

I. INTRODUCTION

At present, The Reversible computation technique is the most preferred area of research for all power dissipation problems. It has voluminous applications in several areas like quantum computing, computer science, optical computing, nanotechnologies, bio-informatics, signal processing, and low power computation [1]. In digital design, the power dissipation will play a significant role in all the data loss problems. In conventional logic gates, if the total number of integrated components in a chip is increased, obviously the total amount of power is dissipated in that chip is also increased, and then it leads to the data loss in a chip. In 1961 R. Landauers [2] has proved that the Irreversible circuits will generate a maximum amount of heat, it diminishes the circuits life. The conventional logic gates will dissipate the K*T*ln2 joules of energy for 1-bit data. To overcome these power dissipation problems are present in conventional logic gates, in 1973 Charles Bennett [3] has proposed that the circuit is built with reversible gates then we should avoid all power dissipation problems in conventional logic gates then we can design any circuit having very less power dissipation across the circuit. Ideally, Zero power dissipation is possible in reversible gates.

In recent times, it is applied to cryptography [4]. The study of reversible computing is encouraged by advancements in nanotechnology, quantum computing, and the low-power design. The Reversible synthesis is mainly focused on a synthesis of the reversible circuits built with the basic reversible gates of NOT gates, CNOT gates, and the Toffoli gates. The Modern simulations tools are based on the FPGAs have enabled the modeling of reversible circuits [5]. The basic cipher design is designed with the VHDL was described in [6].

Here we proposed the application of an encryption/ decryption of data using reversible logic. The main theme of this work is to design a simple execution of the cipher with the reversible logic circuits. The main key is determined with the cascading of each reversible gate. To determine the encryption/decryption of data is mainly depends on choosing the different types of main keys and substitution with different cascades. For this reason, an RRG is proposed.

II. BASIC REVERSIBLE LOGIC GATES

- ***Delay:*** The time taken to propagate the input to the output of a circuit is simply called a delay.
- ***Ancillary bits:*** It is referred to as the overall inputs bits which are maintaining either constant logic '0' or '1' to acquire the suitable output.
- ***Garbage Output:*** It is referred to as the overall vacant outputs positions are present in the circuit.
- ***Quantum cost:*** The total number of 1-input, 1-output (1x1) and the 2-input, 2-output (2x2) reversible gates which are maintained in the circuit is called as quantum cost.

A. NOT Gate:

It is a 1-input and the 1-output (1x1) reversible gate with an equivalent quantum cost is 0. Fig 1 displays the logic diagram and Fig 1.1 displays the Quantum implementation of a NOT gate.

Revised Manuscript Received on 30 July 2019.
***** Correspondence Author
K. Rajesh, Department of Electronics & Communication Engineering, Sri Venkateswara University, Tirupati, India.
Prof. G. Umamaheswara Reddy, Department of Electronics & Communication Engineering, Sri Venkateswara University, Tirupati, India.

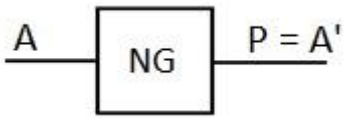

Fig. 1 Logic diagram

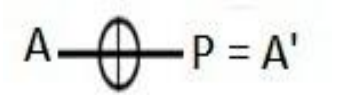

Fig. 1.1 Quantum implementation

B. CNOT (Feynman) Gate: It is a 2-input and the 2-output (2x2) reversible gate with an equivalent quantum cost is 1. Fig 2 displays the logic diagram and Fig 2.1 displays the Quantum implementation of a CNOT gate.

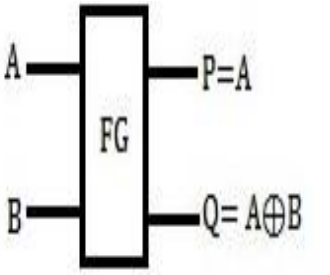

Fig. 2 Logic diagram

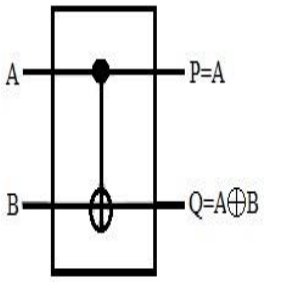

Fig. 2.1 Quantum implementation

C. Toffoli Gate: It is a 3-input and the 3-output (3x3) reversible gate with an equivalent quantum cost is 5. Fig 3 displays the logic diagram and Fig 3.1 displays the Quantum implementation of a Toffoli gate.

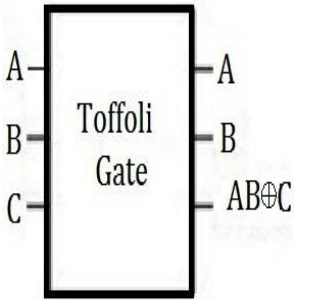

Fig. 3 Logic diagram

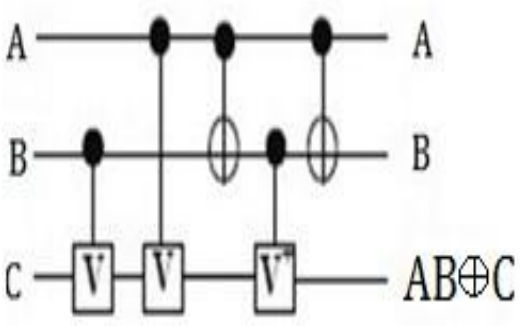

Fig. 3.1 Quantum implementation

D. Fredkin Gate: It is a 3-input and the 3-output (3x3) reversible gate with an equivalent quantum cost is 5. Fig displays the logic diagram and Fig 4.1 displays the Quantum implementation of a Fredkin gate.

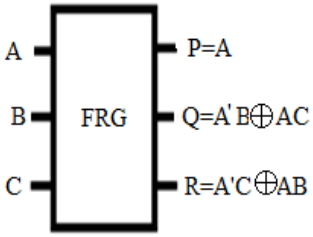

Fig. 4 Logic diagram

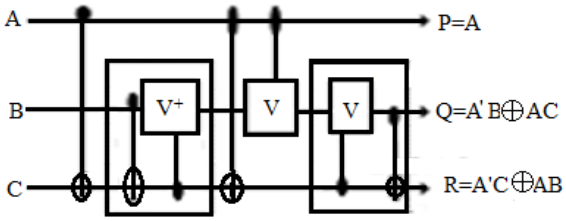

Fig. 4.1 Quantum implementation

III. CONSTRUCTION OF RECONFIGURABLE REVERSIBLE GATE (RRG)

RRG replaces one of the 32 reversible gates from an NCT library in a cipher. That's why in addition to the 4 input bits of transferring data there have to be 5 lines for selecting one of the 32 different types of logic gates. Till now, there is no possibility of synthesizing the 9 input reversible gates. Later considering the different types of logic gates in RRG, a final RRG has proposed in Fig 5 with the reasonably little quantum cost of 79.

The initial three gates G0, G1, and the G2 are select input signals which will further be modified with a 4- input logic gate of G6. In The next stage, three 3-input logic gates of G3, G4, and the G5 are used to control signals of the logic gate G6 which depends on the selection of the specified configuration of constant signals. Therefore the overall execution of a logic gate G6 is decided by the signals 'K'. The logic gates of G7, G8, and the G9 are used to rebuild the constant signals for the logic gates G3, G4, and the G5, and whereas the G10, G11, and the G12 gates are used to retrieving the output signals of Y0, Y1, Y2, and the Y3 are equivalent to the inputs of X0, X1, X2, and the X3. The basic design of RRG using reversible gate is displayed in Fig 6.

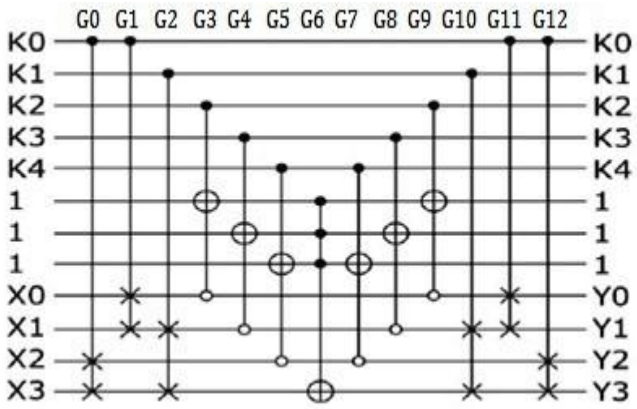

Fig. 5 Reconfigurable Reversible Gate

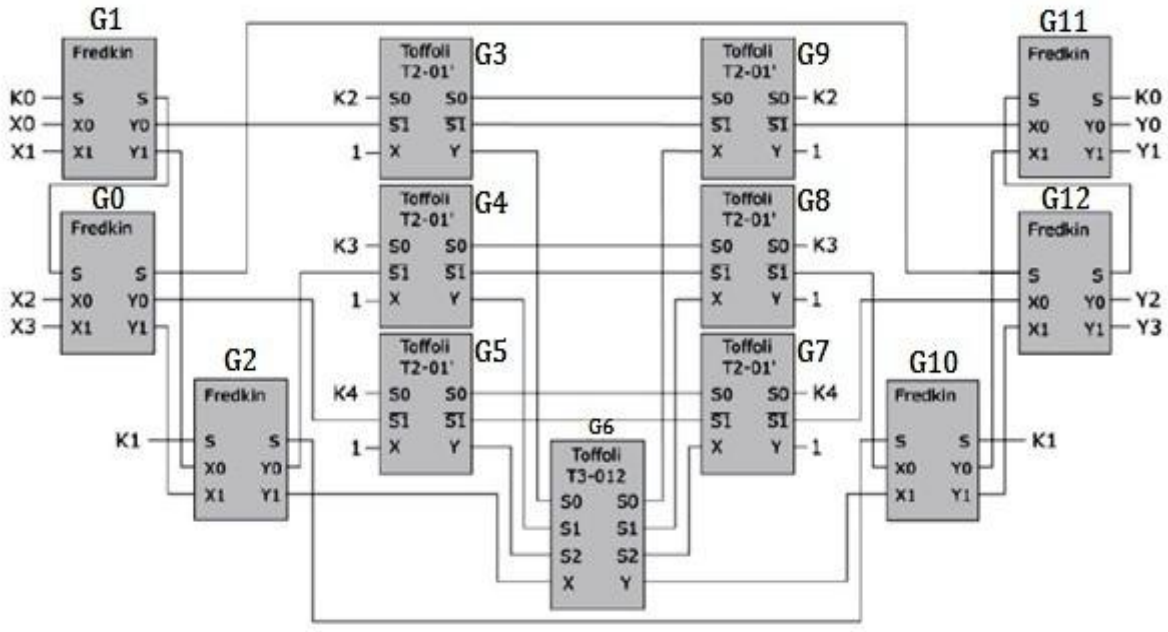

Fig. 6 General organization of Reconfigurable Reversible Gate

IV. OPERATION OF THE ENCRYPTION WITH RRG

The basic thought of a cipher structure is constructed with reversible gates is proposed in [7]. Fig 7 will display the Basic scheme of cipher for Encryption/Decryption of a data. Here, the plain text, main key, and the cipher text are the main keywords which were used in the complete encryption/decryption process. The plain text is nothing but whatever the data we have transmitted secretly. The cipher text is a piece of original information with encrypted form and the main key is used to decryption of the corresponding data whatever the data we are transmitted from the transmitting side. The main key is highly confidential, if once it is revealed to any unauthorized persons; they will access all the encrypted data. Finally, with the use of the main key, we can decrypt the original information. The step by step procedure for converting the Plaintext to a Cipher text with RRG's is

Step 1: Conversion of Plaintext to a cipher text with the RRG's.
Step 2: Main key register for converting a cipher text to the Main key with the use of flip-flops built from Reversible gates.
Step 3: Conversion of Cipher text to Plaintext with the RRG's.

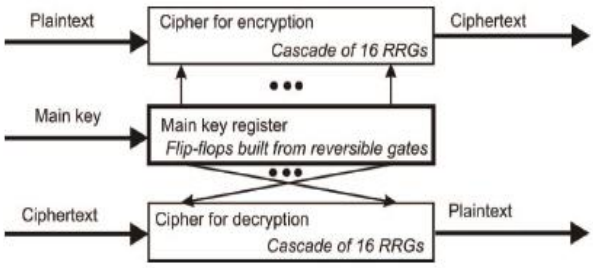

Fig. 7 Basic scheme of cipher for Encryption and Decryption of a data

It's already proved in [8-9] that the optimal logic circuits for any of 16! (Equals to over 1013*2) requires at most fifteen 4-bit input gates. Fig 7 displays an implementation of 4-bit cipher using cascading of the reversible gates. This circuit having 80 inputs of the key with the corresponding input data denoted by K, which are sub-divided into different groups with the 5 inputs in all of them. To configure the i^{th} RRG gate, a 5-line any group of K [(5*(i+1) – 1):5*i] is used.

For controlling the next gate, all the key inputs K is to be transferred to the outputs so that it can be reused. The complete decryption of a main key register and circuit modifications of the contents in encryption and decryption are previously proposed.

V. SIMULATION RESULTS OF CIPHERS

The two 4-bits ciphers, 5- bit key, and the main key register are used for the encryption/decryption of information. Here, we proposed the implementations of 4-bit cipher using cascading of the reversible gates are displayed in Fig 8. The simulation results of 4- bit input data of both encryption/decryption shown in Fig 8 and 9 respectively.

The simulation results of 4-bit input data of Encryption shown in Fig 9. The Ci is '111', Co is '111' are the input and output cipher texts respectively. K is '11001', Ko is '11001' are the input and output keys respectively. X is '0011', Y is '0011' are the input and output messages respectively, which is encrypted from the transmitting side.

The simulation results of 4-bit input data of Decryption shown in Fig 10. The Ci is '111', Co is '111' are the input and output cipher texts respectively. K is '11001', Ko is '11001' are the input and output keys respectively. X is '0011', Y is '0011' are the input and output messages respectively, which is Decrypted from the receiving side.

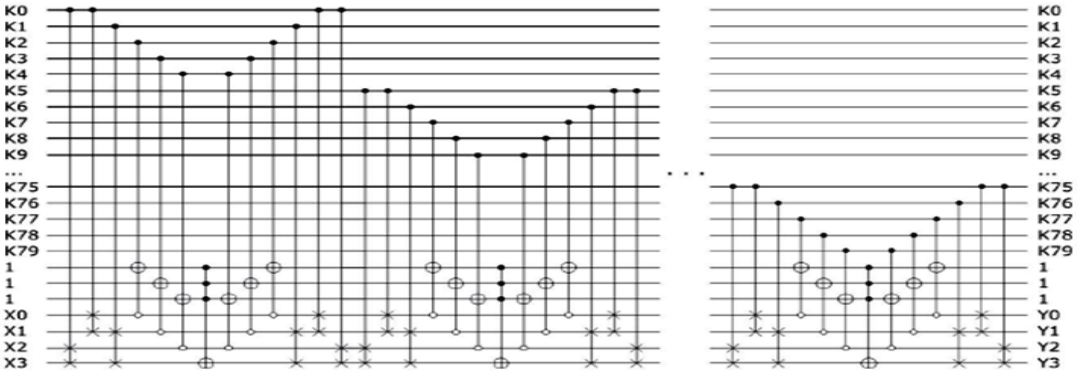

Fig. 8 Implementation of 4-bit cipher using cascading of the reversible gates

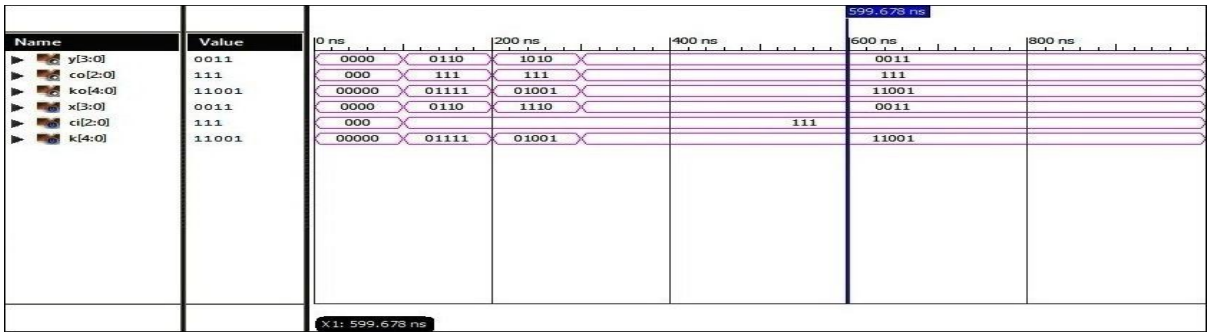

Fig. 9 Simulation results of ENCRYPTION

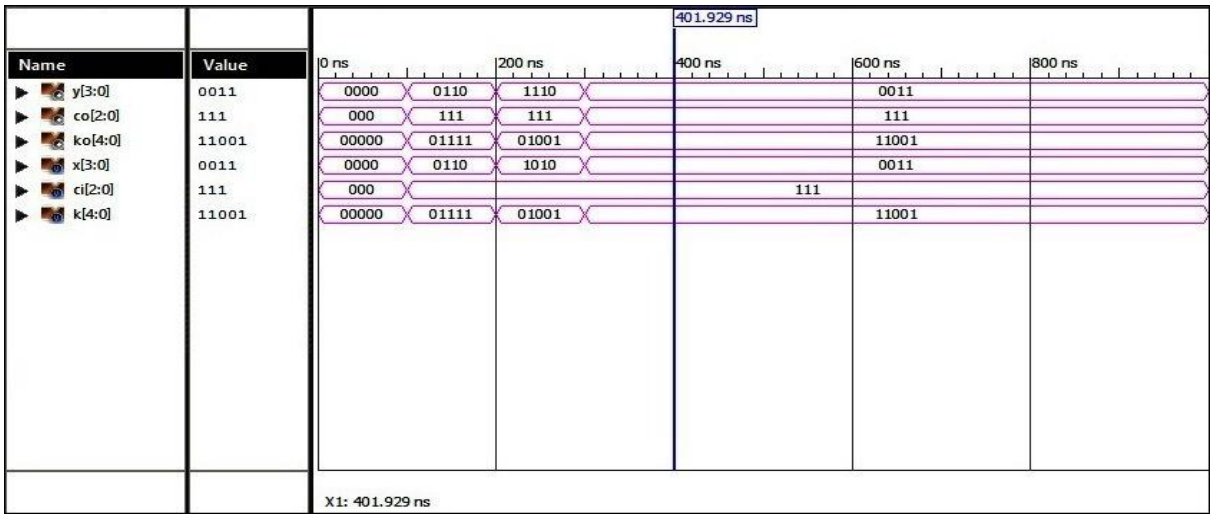

Fig. 10 Simulation results of DECRYPTION

Table I displays the analysis of both Encryption and Decryption processes. The gate count is 13, Constant inputs are 3, Garbage output is 0, Quantum cost is 79 and the Delay is 167.957ns which is same for both the encryption and decryption process because the implementation of the encryption structure is always similar to the decryption.

Table I: Analysis of Encryption and Decryption

S. No	Design	Total Number of Gates	Number Constant inputs	Number Garbage outputs	Quantum cost	Delay
1	Encryption	13	3	0	79	167.957ns (98.425ns logic, 69.532ns route)
2	Decryption	13	3	0	79	

VI. CONCLUSIONS & FUTURE SCOPE

In this work, we proposed an optimized design of simple RRG with the use of basic reversible gates of NOT, CNOT, Toffoli, and Fredkin gates. The simulation results of a cipher are presented and the gate count, constant inputs, delay, quantum cost, and the garbage outputs are also calculated. The entire Simulation and synthesis process is successfully done with the Xilinx ISE 14.7 version and it is dumped on the FPGA Zynq board. The complete encryption/decryption processes of a data will completely depend on the RRG and it is designed with using 13 reversible gates. Might be in future the design of RRG may be more optimized with the new reversible gates. Obviously, the total gate count is reduced and it leads to reduce the quantum cost and the delay of the circuit.

REFERENCES

1. A.De Vos, Berlin 2010, "Reversible computing fundamentals, quantum computing and applications", Wiley-VCH.
2. R.Landauer, 1961, "Irreversibility and heat generation in the computational process", IBM Journal of Research. pp. 183-191.
3. C.H.Bennett and R.Landauer, "The fundamentals physical limits of computation".
4. H.Thapliyal and M.Zwolinski, 2006, "Reversible logic to cryptographic hardware: a new paradigm", 49th Int. Conf. on Circuits and Systems. pp. 342-346.
5. M.Pawlowski and A.Skorupski, 2010, Design of Complex Digital Devices, WKL and Warsaw.
6. A.Skorupski, M.Pawlowski, K.Gracki, and P.Kerntopf, 2012, "FPGA based modelling of encryption systems implemented in reversible logic", Vol. 58, pp. 620-622.
7. K.Datta, V.Shrivastav, I. Sengupta, and H. Rahaman, 2013 "Reversible logic implementation of AES algorithm," Int. Conf. on Design and Technology of Integrated Systems in Nanoscale, pp.140-144.
8. O.Golubitsky and D.Maslov, 2012, "A study of optimal 4-bit reversible Toffoli circuits and their synthesis," IEEE Trans. on Comp, Vol. 61, pp.1341-1353.
9. M.Szyprowski and P.Kerntopf, 2012, "A Study of Optimal 4-bit Reversible Circuit Synthesis from Mixed-Polarity Toffoli Gates," IEEE Conf. on Nanotechnology.

AUTHORS PROFILE

K. Rajesh, Research Scholar, Department of Electronics and Communication Engineering, Sri Venkateswara University, Tirupati. He is B.Tech in Electronics and Communication Engineering from JNT University, Kakinada, and M.Tech in VLSI system design from JNT University, Kakinada. He has Teaching Experience of 3 Years has 6 technical publications. His areas of Interest are Low-Power VLSI and Embedded systems.

Professor G. Umamaheswara Reddy is received B.Tech degree in Electronics and Communication Engineering, M.Tech in Instrumentation & Control Systems, and obtained Ph.D. from Sri Venkateswara University, Tirupati. He is a member of the ISTE, IE, and BMSI. Currently, he is a Professor at Department of Electronics and Communication Engineering, Sri Venkateswara University, Tirupati, Andhra Pradesh. He has a teaching experience of more than 20 years and has 23 technical publications in national/international journals. His areas of interest includes VLSI, Signal processing and Bio-medical signal processing.